SYSTEM AND METHOD FOR MONITORING DATA TRAFFIC ON A NETWORK

BACKGROUND OF THE INVENTION

1. Field of Invention

[0001] The invention relates to a network monitoring device and method for monitoring and distributing network traffic data to terminals of a network.

2. Description of Related Art

[0002] Currently, network service providers operate data networks that permit a plurality of network users to communicate with each other. The network users can be roughly divided into two groups: servers and individual users. Generally, the servers are terminals connected with the network that provide a service to their clients, such as selling products or providing information. The individual users are terminals that can be used by private individuals for communicating over the network, such as by e-mail, IP telephony, or video conferencing. A portion of the individual users may also be clients of the servers that use the network to purchase products and services from the servers.

[0003] Presently, network service providers are able to collect network traffic data for maintenance and management of their networks. The network traffic data includes information about the use of the network by all the network users connected with the network. The network traffic data is usually acquired over relatively large periods of time, and then the aggregated data is analyzed to determine traffic flow patterns. However, traffic on the network is continually changing. New sites are constantly being added to the network while others are being removed, and new networks are continually linking to existing networks.

SUMMARY OF THE INVENTION

[0004] Accordingly, it is an object of the present invention to provide a network monitoring device that monitors a network in order to gather information on the traffic flow generated by network users over the network. The network monitoring device can subsequently distribute network traffic information to subscribers. As the network traffic information is gathered, the network monitoring device can further analyze the information to discern patterns in the traffic flows. A large network service provider, such as AT&T, with access to network traffic data from a large population of network end users and business servers can use the network traffic data to obtain information on

various patterns in the network traffic data flow and related business interests in real-time.

[0005] Knowledge about data traffic flow can be very valuable for businesses and/or individuals that have web sites on a network, such as the Internet. Such data traffic flow information can include information on where, when and what sites are being visited along with data indicating with what volume they are being visited. With such information, network users are able to update their sites or change the presence of their sites to correspond to the actions and desires of individual users on the network. By enhancing sites in real-time based on the network traffic information, the network users will be able to target their sites and attract a certain clientele.

[0006] For example, by analyzing network traffic data, a focused interest of network users in a type of business, such as the flower business, might be discovered. The network traffic data may indicate that a few flower shops are getting a majority of the marketshare of data traffic related to the flower business. From this information, it may be deduced that these businesses are offering some type of deal to attract clients. Furthermore, competitors may visit the heavily traveled sites to determine why the sites are attracting a large marketshare. The businesses that receive the traffic information may be inclined to offer deals to compete with their business competitors. Therefore, these businesses can gain an edge in the market by knowing how the network traffic is behaving at any moment.

[0007] Another example involves the use of advertisements on the network. Usually advertising companies act as a liaison between network sites and companies placing advertisements on those sites. By using the data traffic flow information provided from the analyzed network traffic data, advertising companies can determine which sites are being visited by heavy volumes of network traffic. Additionally, data traffic flow information can indicate a geographical source or origin, such as a county or state, from which the network traffic is being generated. Therefore, advertisements can be strategically and more accurately placed on selected sites of the network. As a result, the click-through rate of those advertisements will increase and the impression the advertisements have on network users will be maximized.

[0008] Accordingly, the present invention provides methods and systems for obtaining network traffic information, analyzing the data and displaying the analyzed

data. This can be accomplished in real-time to provide businesses and individuals with the advantage of having immediate analyzed network traffic data.

BRIEF DESCRIPTION OF THE DRAWINGS

[0009] The invention is described in detail with regard to the following figures, in which like elements are referred to with like numerals, and in which:

Fig. 1 is an exemplary block diagram of a network traffic monitoring system in accordance with the present invention;

Fig. 2 is an exemplary block diagram of the network monitoring device shown in Fig. 1;

Fig. 3 is an exemplary data structure for storing network traffic information;

Fig. 4 is a graph showing an exemplary network traffic history;

Fig. 5 is an exemplary data structure for storing subscriber information; and

Fig. 6 is a flowchart outlining an exemplary embodiment of the network traffic monitoring system.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

[0010] Fig. 1 is an exemplary block diagram of a network traffic monitoring system 100 according to the present invention. As shown in Fig. 1, the system 100 includes terminals 102-108, servers 112-118 and a network monitoring device 122 coupled to the network 101 through a communication link 110.

[0011] The terminals 102-108 can be devices of any type that allow for the transmission and/or reception of communication signals and allow a subscriber to connect to and use a network's capacity, features and services, and access content available through the network. For example, the terminals 102-108 may include land-line telephones, smart or computer-assisted televisions, digital set-top audio/video decoders, personal digital video recorders, screen-equipped web phones, voice and video telephone sets, streaming audio and video media players, integrated intelligent digital television receivers, personal computers, workstations, thin-client network computers, radios, personal digital assistants, PCS/cellular wireless voice and Internet phones, mobile satellite receivers, GPS receivers, automated teller machines, or any combination of these. For the purposes of the present disclosure, it will be assumed that terminals 102-108 are personal computers.

[0012] The servers 112-118 provide services, such as sales of products, services or information, to terminals 102-108 over the network 101. Each server 112-118 may also independently gather information, for example from other networks or databases, for each terminal 102-108 that uses its services. The servers 112-118 can include one or more computers, databases and the like connected with the network that provide websites, electronic commerce, informational services, search engines, and the like.

[0013] The terminals 102-108, servers 112-118 and the network monitoring device 122 are in communication with network 101 through communication links 110. These communication links 110 can be any type of connection, wired or wireless, that allows for transmission of information. Some examples include, but are not limited to, multiple twisted pair cable, digital subscriber lines (DSL), coaxial cable, optical fiber, RF cable modems, over-the-air radio frequency, over-the-air optical wavelength (e.g., infrared), local area networks, wide area networks, intranets, virtual private networks, cable TV, terrestrial broadcast radio or television, satellite transmission, simple direct serial/parallel wired connections, or the like.

[0014] The network 101 may be a single network or a plurality of networks of the same or different types. For example, the network 101 may include a local telephone network in connection with a long-distance network (such as an AT&T long-distance telephone network). Further, the network 101 may be a data network or a telecommunications network or video distribution network (e.g., cable, terrestrial, broadcast or satellite) network in connection with a data network. Any combination of telecommunications, video/audio distribution and data networks, whether a global, national, regional, wide-area, local area or in-home network, may be used without departing from the spirit and scope of the present invention. For the purposes of discussion, it will be assumed that the network 101 is a data network.

[0015] Network monitoring device 122 monitors the network 101 and gathers network information, such as data traffic being transmitted on the network 101. For example, the network monitor device 122 can monitor communications between the terminals 102-108, between terminals 102-108 and servers 112-118, and between the servers 112-118. The network monitoring device 122 can further monitor communications across the network 101 which only traverse the network 101 (i.e., only travel over the network and are not directed to any of the terminals 102-108 and/or the

servers 112-118 connected with the network 101). Further, the network monitoring device 122 can monitor any communication that begins from any of the terminals 102-108 and/or servers 112-118 and are directed to another terminal outside the network 101. In short, the network monitoring device 122 can monitor any communications that are transmitted across the network 101.

[0016] To monitor the communications transmitted on network 101, the network monitoring device 122 can examine a header portion of each of the communications, such as an IP header. For example, the IP header can contain an originating and destination terminal address, along with a time that the communication was placed. The information can be extracted from each of the communications and collected in a memory. Once collected in the memory, the network monitoring device 122 can analyze the data to determine any patterns in the aggregate network traffic flow. For example, the network monitoring device 122 can determine if numerous data communications are being transmitted to or from a particular server 112-118 or terminal 102-108 within a period of time. The transmission of numerous communications between the terminals 102-108 and a particular server over a period of time can constitute a traffic pattern. Once a pattern is determined, the network monitoring device 122 may notify any subscribers to which the traffic pattern may be of particular interest.

[0017] The network monitoring device 122 may be an independent unit coupled to the network 101 (as shown), or it may be distributed throughout the network 101. For example, the network monitoring device 122 may be resident in the system 100 or equipment located in the various telephone central office, cable system head-end or distribution hub, satellite up-link, broadcast studio, server complex, or data center premises which are distributed throughout and coupled to the network 101. Any configuration that permits the monitoring of data traffic over the network 101 may be used without departing from the spirit and scope of the present invention.

[0018] Fig. 2 is an exemplary block diagram of a network monitoring device 122. The network monitoring device 122 includes a controller 200, a network interface 202, a network traffic memory 204 and a subscriber database 206. As shown, the above components can be coupled together through a control/signal bus 212.

[0019] In operation, the controller 200 can monitor the communication traffic on the network 101 via network interface 202. The network interface can be coupled to

the network 101 or numerous nodes (not shown) of the network via the network 101 itself or a separate network, such as a control network. For example, the controller 200 can monitor the communications of individual terminals 102-108 to and from various websites offered by the servers 112-118. As described above, data concerning the communications of a particular terminal 102-108 can be collected from a header portion of the communication that is used to direct a communication from an originating terminal to a destination terminal.

[0020] After monitoring a communication, the controller 200 can further collect and store any network data traffic in the network traffic memory 204. At this point, the network traffic data can be stored in a sorted manner in order to group network traffic directed to particular servers, 112-118, websites, or types of websites together. Furthermore, data traffic originating from a particular terminal 102-108 or group of terminals 102-108 can be grouped together in the network traffic memory 204. Alternatively, the network traffic data can be stored without any organization to be sorted at a later time.

[0021] One example of operation could be to use the network monitoring device 122 in order to assist subscribers in real-time traffic-based business planning. For example, a subscriber may request that a network service provider monitor the servers or web sites of certain businesses in a particular category, such as businesses related to the sales of flowers. For the purpose of this example, assume that servers 112-118 all operate websites related to the sales of flowers over the network 101. Furthermore, assume that on this particular day, the server 112 is selling roses at one-half (½) of the price that servers 114-118 are selling the same type of roses. Finally, assume that servers 116 and 118 subscribe to a service of the network monitoring device 122 that provides servers 116 and 118 with network traffic information of the servers in the flower business (i.e., servers 112-118).

[0022] Assume that over the course of the same business day, the network monitoring device 122 observes that, of the servers 112-118, server 112 is receiving a large volume of data traffic relative to that of servers 114-118. In response, the network monitoring device 122 can notify the subscribers, servers 116 and 118, of the increased or disproportionate traffic flows. Based on the information, the operators of servers 116 and

118 may be inclined to investigate the server 112's website to see why the server 112 has such a high traffic flow.

[0023] From the investigation, the servers 116 and 118 may determine that the server 112 is offering roses at half price, and that is why the server 112 is experiencing high traffic flow. In response, the servers 116-118 may also offer roses at half price in order to compete with server 112. Accordingly, once the information has been disseminated, servers 116 and 118 should experience increased traffic flow.

[0024] Because the server 114 will not be notified of the increased volume in traffic, server 114 may remain unaware that servers 112, 116 and 118 have now lowered their price of roses by one half. Accordingly, server 114's marketshare may decrease even more as a result of server 114's limited knowledge of the network market environment.

[0025] It is to be understood that not only servers 112-118 can subscribe to the data traffic monitoring service. For example, the users of the terminals 102-108 may wish to subscribe to a service that monitors the traffic flows of certain categories of business or web sites. In the above example, if terminal 102 had subscribed to the traffic flow data of the servers 112-118 that were in the business of selling flowers, the user of terminal 112 would have been notified of the disproportionate traffic flow to server 112 and therefore could have further investigated and possibly benefited from the sale price of roses.

[0026] While, in the above examples, the users of the terminals 102-108 and servers 112-118 are described as having to monitor the traffic flow data and decide whether to further investigate and determine the cause of traffic data, it is to be understood that this function may be automated, for example by various software applications, without departing from the spirit and scope of the present invention. Further, the decision of whether or not to change one's presence on the network, such as the lowering of prices in the above example, may also be automated in a like manner without departing from the spirit and scope of the present invention.

[0027] In another example, the traffic flow data can be used for the strategic placement of advertisements on web sites in order to maximize the click-through rates or viewing of the advertisements. For example, an advertisement brokerage company that is responsible for the placement of advertising clients' advertisements on web sites or the

like for numerous advertising clients can subscribe to the network traffic service in order to receive traffic flow information over the entire network 101. The advertisements may be such that they may be interchangeably displayed on various web sites.

[0028] In operation, the advertisement brokerage company can selectively display the advertisement of their clients on web sites that are experiencing a heavy volume of data traffic. For example, while a site is dormant (i.e., receiving less than five visitors per hour), the advertisement brokerage company may choose not to display any advertisements, since very few people will view the advertisements. Further, it may not be cost-effective to rent space on the web site if very few people are to view the advertisement. However, if the advertisement brokerage company receives data traffic from the network monitoring device 122 that a site has a very heavy traffic flow (i.e., 100+ visitors per hour), then the advertisement brokerage company may decide to display their advertising clients' advertisements on the web site.

[0029] For example, the increase in traffic flow through the site may be due to a special event being held at the site, such as a broadcast of a sporting event. In any event, the network monitoring device 122 will recognize the increased traffic flow and the subscribing advertisement brokerage company will be able to maximize the viewability of their advertising clients' advertisements by targeting this site during the increased traffic flow. Subsequently, once the network monitoring device 122 determines that the traffic flow to the particular web site has once again decreased, the advertisement brokerage company can once again decide not to display their advertising clients' advertisements at the web sites. Accordingly, the network traffic data can be used to take advantage of the often wildly fluctuating and temporal nature of traffic on the network.

[0030] In another example, the network monitoring device 122 can be used to accomplish real-time traffic-based targeting, where advertising is directed at specific sites when traffic is determined to be heavy at that site. For example, if a temporary increase in traffic is monitored at a site that is related to politics, then the network monitoring device 122 can report to an advertisement brokerage company, for example, that there is an increase in traffic to the site that generally relates to politics. Based on this information, the advertisement brokerage company can direct advertisements to this site, and the advertisements can be related to the content of the site, in this case, for example, political ads.

[0031] Further, in the above example, the network monitoring device may determine that the data traffic is from the same geological area, such as a state or county. Based on this information, the advertisement brokerage company may further focus the display of advertisements particularly to local clients, such as a store that is mainly located within the identified county or state.

[0032] Fig. 3 is an exemplary data structure 300 of the network memory 204 that stores information related to communications on the network 101. Field 302 contains server terminal IDs. For the purposes of this disclosure, the terminal IDs correspond to the reference numerals shown in Fig. 1. For example, the server terminal ID 112 corresponds to server 112.

[0033] Field 304 contains the corresponding terminal IDs of the visiting terminals. For example, these can be terminals that are currently connected with the server via the network 101. As described above, this data can be derived from a header portion of a communication traveling across the network. For the purposes of this disclosure, the visiting terminal IDs correspond to the reference numerals shown in Fig. 1.

[0034] Field 306 contains a current rate at which the corresponding server identified in field 302 is receiving visitors. The rate may be calculated based on a number of visitors connecting with the server over a predetermined period of time. For example, as shown in field 306, the rate is described in terms of visitors per hour.

[0035] It is to be understood that Fig. 3 is an exemplary data structure of the network traffic memory 204, and that various other fields may be added without departing from the spirit and scope of the present invention. For example, referring to Fig. 4, the network traffic history of a particular server or terminal may be stored over a period of time. For example, a data traffic pattern over a 24-hour period may be stored and analyzed to determine when the site historically receives more or less traffic. Additionally, the 24-hour periods or days may be stored so that traffic patterns over a week or month can be analyzed or determined.

[0036] As shown in Fig. 4, it can be seen from the graph that on weekdays, the server corresponding to server terminal ID 112 generally receives its heaviest data traffic flow at 10 a.m. and 7 p.m. Further, as can be seen, on the weekend a server

corresponding to server terminal ID 112 receives a generally steady flow of traffic between the period of 8 a.m. and 8 p.m.

[0037] Fig. 5 is an exemplary data structure 500 of the subscriber database 206. Field 502 contains a subscriber ID. This subscriber ID can be the IP address of each of the servers 112-118. For example, the subscriber ID 112 corresponds to the server 112, as shown in Fig. 1.

[0038] Field 504 contains a service type ID. The service type ID can identify the area of traffic flow interest in which the corresponding subscriber in field 502 is interested. For example, subscriber 112 is interested in receiving traffic flow data related to e-commerce. More particularly, subscriber 112 is interested in receiving data flow traffic pertaining to e-commerce relating to flowers.

[0039] As shown in field 504, the subscriber 114 is interested in receiving data flow traffic so that the server 114 may place ads that are directed at an individual visiting server 114's site. For example, if the controller 200 determines that terminal 102-108 with users having a particularly specialized interest, such as travel, are visiting server 114's website, then server 114 will display advertisements related to travel. Alternatively, if the data traffic or an individual of the data traffic is viewing terminal 114's website, and it has been determined that the visiting terminals have an interest in sporting goods, then the server 114 can display advertisements directed toward the sporting goods, or sporting stores or the like.

[0040] In operation, the controller 200 monitors the network 101 via network interface 202. For example, assume that terminal 102 initiates a communication with server 112 via network 101. As the communication travels across the network 101 via a plurality of routers (not shown), the network monitoring device 122 can receive information on the communication. For example, the network monitoring device can extract the address of the terminal 102, the address of the server 112 and a time that the communication was placed from a header portion of the communication.

[0041] Once the network monitoring device 122 has received the information, the information may then be stored in the network traffic memory 204. As numerous communications are placed on the network 101, the network monitoring device 122 may continually monitor and collect data on the communications.

[0042] Figure 6 is a flowchart outlining the exemplary process for monitoring data traffic on a network. In step 600, the process begins. In step 602 the network is monitored for any communications that may be travelling on or across the network. The process then proceeds to step 604.

[0043] In step 604 a determination is made as to whether network traffic is traveling on or across the network. If a data communication is detected on the network, then the process proceeds to step 606; otherwise, the process returns to step 602 where the network is continued to be monitored.

[0044] In step 606, information contained in the traffic travelling on the network is gathered. The information may include an originating address, a destination address, and a time of transmission for the communication. Furthermore, the information may be extracted from a header portion, such as an IP header portion, of a data communication travelling across the network. The process then proceeds to step 608.

[0045] In step 608, the traffic information can be stored in a memory. In step 610 a pattern recognition algorithm can be applied to the stored memory. The pattern recognition may organize the data traffic in any number of ways in order to recognize data traffic flows across the network. For example, the data traffic may be organized by destination terminal. In other words, all data traffic being sent to a particular terminal may be grouped together as a traffic flow. The process then proceeds to step 612.

[0046] In step 612, any traffic flow patterns that are recognized in step 610 can be reported to the subscribers. The subscriber may only receive information regarding patterns which are relevant to the subscriber. Control then returns to step 602 where the process can begin again.

[0047] As shown in Fig. 2, the method of this invention is preferably implemented on a programmed processor. However, the network monitoring device 122 can also be implemented as part of a switch or a stand-alone or a general purpose or a special purpose computer, a programmed microprocessor or microcontroller and peripheral integrated circuit elements, an Application Specific Integrated Circuit (ASIC), or other integrated, hardware electronic or logic circuit such as a discrete element circuit, a programmable logic device such as a PLD, PLA, FPGA, or PAL, or the like. In general, any device on which exists a finite state machine capable of implementing the

flowcharts shown in Fig. 6 can be used to implement the network monitoring device 122 functions of this invention.

[0048] While this invention has been described in conjunction with the specific embodiments thereof, it is evident that many alternatives, modifications, and variations will be apparent to those skilled in the art. Accordingly, preferred embodiments of the invention as set forth herein are intended to be illustrative, not limiting. There are changes that may be made without departing from the spirit and scope of the invention.